INDEX BY AUTHOR
CRYPTOLOGIA
VOLUME 21 (1997)

Thomas R. Cain and Alan T. Sherman
237 How to Break Gifford's Cipher
C. C. Chang, J. K. Jan, and H. C. Kowng
55 A Digital Signature Scheme Based Upon the Theory of Quadratic Residues
H. F. Chau and H.-K. Lo
139 One-Way Functions in Reversible Computations
Andrew Clark and Ed Dawson
129 A Parallel Genetic Algorithm for Cryptanalysis of the Polyalphabetic Substitution Cipher
Paul Constance
71 How Jim Bamford Probed the NSA?
Ed Dawson and Andrew Clark
129 A Parallel Genetic Algorithm for Cryptanalysis of the Polyalphabetic Substitution Cipher
C. A. Deavours
193 Lobsters, Crabs, and the Abwehr ENIGMA
Ralph Erskine
42 The First Naval ENIGMA Decrypts of World War II
378 Letter to the Editor
Caxton C. Foster
350 Drawbacks of the One-Time Pad
H. Paul Greenough
353 Cryptanalysis of the Swedish NC-9: A Known-Plaintext Approach
Jacques B. M. Guy
51 The Distribution of Signs c and o in the Voynich Manuscript: Evidence for a Real Language?
Tzonelih Hwang and Narn-Yih Lee
327 On the Security of Park *et al.*'s Key Distribution Protocol for Digital Mobile Communications
J. K. Jan, C. C. Chang, and H. C. Kowng
55 A Digital Signature Scheme Based Upon the Theory of Quadratic Residues
Stephen J. Kelley
289 The SIGCUM Story: Cryptologic Failure, Cryptologic Success
Neal Koblitz
317 Cryptography as a Teaching Tool
H. C. Kowng, C. C. Chang, and J. K. Jan
55 A Digital Signature Scheme Based Upon the Theory of Quadratic Residues

Louis Kruh
75 Reviews and Things Cryptologic
110 Reviews and Things Cryptologic
218 Reviews and Things Cryptologic
335 Reviews and Things Cryptologic
Narn-Yih Lee and Tzonelih Hwang
327 On the Security of Park *et al.*'s Key Distribution Protocol for Digital Mobile Communications
H.-K. Lo and H. F. Chau
139 One-Way Functions in Reversible Computations
Michael van der Meulen
200 Bundeswehrtarnverfahren
Peter Pesic
1 François Viète, Father of Modern Cryptanalysis – Two New Manuscripts
Aviel D. Rubin
110 An Experience Teaching a Graduate Course in Cryptography
George Sassoon
93 British Company Makes PGP Easier to Use
David Schimmelpenninck van der Oye
39 A First Look at Russia's Codebreakers – A Book Review
Norman Scott
149 Solving Japanese Naval Ciphers 1943–45
Alan T. Sherman and Thomas R. Cain
237 How to Break Gifford's Cipher
From the Archives
30 The BRUSA Agreement of May 17, 1943
158 British Economic Espionage
165 German Wireless Intercept Organization
368 Radio Intelligence and Security

382 Index by Author - Volume 21 (1997)